REMARKS

Claims 1-4, 6-16 and 18-24 are pending in the present application. By this response, claims 1-3, 7-15, 19, 20 and 22-24 are amended and claims 5 and 17 are canceled. Claims 1, 8, 11-13, 20, 23 and 24 are amended to incorporate subject matter similar to canceled claims 5 and 17. Additional support for the amendments to claims 1-3, 7-15, 19, 20 and 22-24 may be found at least on page 12, lines 26 to page 14, line 3. Claims 2 and 9 are further amended to correct minor informalities. Reconsideration of the claims in view of the above amendments and following remarks is respectfully requested.

Amendments are made to the specification to correct errors and to clarify the specification. No new matter is added by any of the amendments to the specification.

I. Examiner Interview

Applicants thank Examiner Nguyen for the courtesies extended Applicants' representatives during the June 8, 2004 telephone interview. During the interview, Examiner Nguyen provided clarification of the rejections based on the McDonough and Kristol references. Applicants have made amendments to the claims based on the information provided by Examiner Nguyen. Therefore it is Applicants understanding that, pending an update search by Examiner Nguyen, the present claims are now in condition for allowance. The substance of the interview is summarized in the remarks of Section II, which follows.

II. 35 U.S.C. § 103, Alleged Obviousness, Claims 1-24

The Office Action rejects claims 1-24 under 35 U.S.C. § 103(a) as being allegedly unpatentable over McDonough et al. (U.S. Patent No. 5,991,878) in view of D. Kristol et al. (Network Working RFC 2109, "HTTP State Management Mechanism", 13 pages, February 1997). This rejection is respectfully traversed.

As to claim 1, the Office Action states:

As per **claim 1**, McDonough teaches a method in a data processing system for removing information, the method comprising: receiving a selection of information for removal from a history (e.g., cookies) generated by a browser, wherein the selection is received prior to a browser session (Fig. 2A, *step 1010*, col. 1, line 35-36; col. 3, lines 14-16); and the automatic removal of the history based on a limited duration (col. 1, lines 45-47, *in accordance with an expiration time indication during a single browser session*).

However, McDonough does not specifically teach the automatic removal of the information from history using the selection without requiring a user input responsive to a termination of the browser session.

Kristol teaches the automatic removal of the information from the history without requiring a user input by setting the expiration to zero causing the cookie to be discarded immediately(Page 5, Section 4.2.2) or setting the default behavior to discard the cookie when the user exits the session (Page 7, Section 4.3.1).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of the invention to implement the method as taught by McDonough to include Kristol's teaching of removing the information from the history upon terminating the browser session. One skilled in the art would have been motivated to do so because the user does not have to remember to manually clear confidential data since the system automatically clears the confidential information so that each session will begin anew, thus protecting the privacy of the user (Page 16, Section 7.1).

Office Action dated March 12, 2004, page 3.

Claim 1, which is representative of the other rejected independent claims 11, 13 and 23 with regard to similarly recited subject matter, reads as follows:

1. A method in a data processing system for removing information, the method comprising:

receiving a selection of confidential information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser;

identifying data elements, within the history, that correspond to the confidential information that has been selected; and

responsive to a termination of the browser session, automatically removing the selected confidential information from the history without requiring further user input upon termination of the browser session, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history. (emphasis added)

McDonough and Kristol, taken alone or in combination, fail to teach or suggest receiving a selection of confidential information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is

composed of multiple data elements generated by a browser, identifying data elements, within the history, that correspond to the confidential information that has been selected, and responsive to a termination of the browser session, automatically removing the selected confidential information from the history without requiring further user input upon termination of the browser session, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history.

McDonough is directed to controlling access to information in a distributed computing system. In the McDonough system, a request for the information is received and is accompanied by encrypted session state data. Based on the encrypted session state data, it is determined whether to pass the request on to a source of the information. In a memory buffer, old data is replaced by overwriting with a unique identifier. After the memory buffer has received new data and a procedure has been executed for copying the contents of the memory buffer to a destination, it is determined whether the unique identifier may be found at the destination.

Thus, in the system of McDonough, the request for the information is received and is accompanied by encrypted session state data, after the browser session has been started. The Office Action claims that McDonough teaches receiving a selection of confidential information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser, at Figure 2A, step 1010, column 1, lines 35-36 and column 3, lines 14-16, which are shown and read as follows:

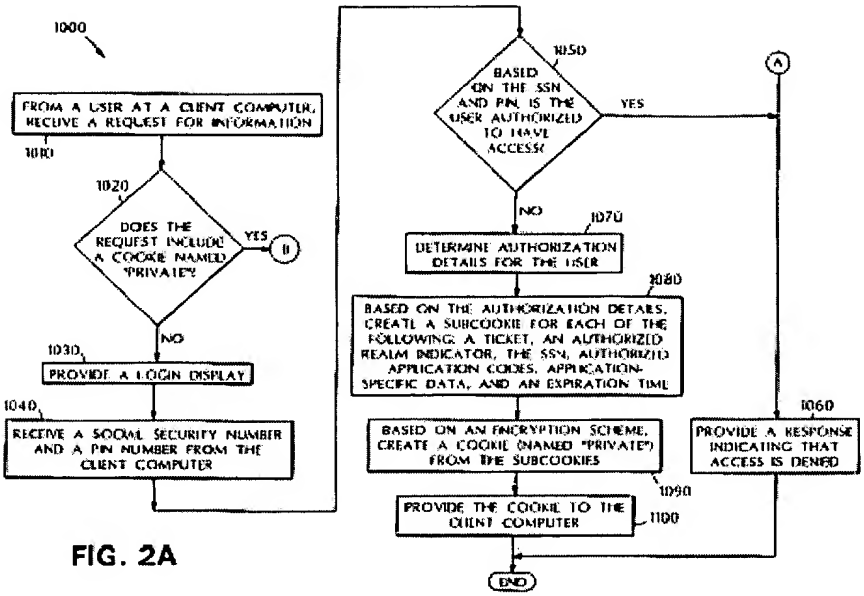

FIG. 2A

(Figure 2A)

> The method includes receiving a request (for the information) accompanied by encrypted session state data (e.g., provided as a generic cookie), and, based on the encrypted session state data, determining whether to pass the request to a source (e.g., a server computer) of the information.

(Column 1, lines 35-36)

> First, a URL-based request for information is received by the server system software from the browser software (step 1010).

(Column 3, lines 14-16)

In these sections, McDonough is merely describing that, during a browser session and prior to displaying the requested information a determination is made as to whether the user has access privileges to the requested information. The URL-based request for information is not historical information but information the user is requesting to view. There is nothing in these sections, or any other section of McDonough, that teaches or suggests receiving a selection of confidential information for removal from a history generated by a browser, wherein the selection is received prior to a browser session.

Furthermore, McDonough does not teach responsive to a termination of the browser session, automatically removing the selected confidential information from the history without requiring further user input upon termination of the browser session, wherein only the selected confidential information is removed without destroying the

integrity of other portions of the history. As shown above, McDonough fails to teach receiving a selection of confidential information for removal from a history generated by a browser. Therefore, McDonough does not teach responsive to a termination of the browser session, automatically removing the selected confidential information from the history. Additionally, the Office Action acknowledges that McDonough does not teach or suggest automatically removing the information from the history using the selection without requiring a user input. Applicants agree that McDonough does not teach this feature. However, the Office Action alleges that Kristol teaches this feature at Page 5, Section 4.2.2 and Page 7, Section 4.3.1, which reads as follows:

> 4.2.2 Set-Cookie Syntax
>
> The syntax for the Set-Cookie response header is
>
> ```
> set-cookie    =     "Set-Cookie:" cookies
> cookies       =     1#cookie
> cookie        =     NAME "=" VALUE *(";" cookie-av)
> NAME          =     attr
> VALUE         =     value
> cookie-av     =     "Comment" "=" value
>               |     "Domain" "=" value
>               |     "Max-Age" "=" value
>               |     "Path" "=" value
>               |     "Secure"
>               |     "Version" "=" 1*DIGIT
> ```
>
> Informally, the Set-Cookie response header comprises the token Set-Cookie:, followed by a comma-separated list of one or more cookies. Each cookie begins with a NAME=VALUE pair, followed by zero or more semi-colon-separated attribute-value pairs. The syntax for attribute-value pairs was shown earlier. The specific attributes and the semantics of their values follows. The NAME=VALUE attribute-value pair must come first in each cookie. The others, if present, can occur in any order. If an attribute appears more than once in a cookie, the behavior is undefined.
>
> NAME=VALUE
> Required. The name of the state information ("cookie") is NAME, and its value is VALUE. NAMEs that begin with $ are reserved for other uses and must not be used by applications.
>
> The VALUE is opaque to the user agent and may be anything the origin server chooses to send, possibly in a server-selected printable ASCII encoding. "Opaque" implies that the content is of interest and relevance

only to the origin server. The content may, in fact, be readable by anyone that examines the Set-Cookie header.

Comment=comment
Optional. Because cookies can contain private information about a user, the Cookie attribute allows an origin server to document its intended use of a cookie. The user can inspect the information to decide whether to initiate or continue a session with this cookie.

Domain=domain
Optional. The Domain attribute specifies the domain for which the cookie is valid. An explicitly specified domain must always start with a dot.

Max-Age=delta-seconds
Optional. The Max-Age attribute defines the lifetime of the cookie, in seconds. The delta-seconds value is a decimal non-negative integer. After delta-seconds seconds elapse, the client should discard the cookie. A value of zero means the cookie should be discarded immediately.

Path=path
Optional. The Path attribute specifies the subset of URLs to which this cookie applies.

Secure
Optional. The Secure attribute (with no value) directs the user agent to use only (unspecified) secure means to contact the origin server whenever it sends back this cookie.

The user agent (possibly under the user's control) may determine what level of security it considers appropriate for "secure" cookies. The Secure attribute should be considered security advice from the server to the user agent, indicating that it is in the session's interest to protect the cookie contents.

Version=version
Required. The Version attribute, a decimal integer, identifies to which version of the state management specification the cookie conforms. For this specification, Version=1 applies.

(Page 4-5, Section 4.2.2)

4.3.1 Interpreting Set-Cookie

The user agent keeps separate track of state information that arrives via Set-Cookie response headers from each origin server (as distinguished by name or IP address and port). The user agent applies these defaults for optional attributes that are missing:

VersionDefaults to "old cookie" behavior as originally specified by Netscape. See the HISTORICAL section.

Domain Defaults to the request-host. (Note that there is no dot at the beginning of request-host.)

Max-AgeThe default behavior is to discard the cookie when the user agent exits.

Path Defaults to the path of the request URL that generated the Set-Cookie response, up to, but not including, the right-most /.

Secure If absent, the user agent may send the cookie over an insecure channel.

(Page 7, Section 4.3.1)

Kristol is directed to a way to create a stateful session with HTTP requests and responses. It describes two new headers, Cookie and Set-Cookie, which carry state information between participating origin servers and user agents. The method described here differs from Netscape's Cookie proposal, but it can interoperate with HTTP/1.0 user agents that use Netscape's method. While Kristol may teach removal of information when the age of a cookie expires, Kristol does not teach receiving a selection of confidential information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser. Furthermore, Kristol does not teach responsive to a termination of the browser session, automatically removing the selected confidential information from the history without requiring further user input upon termination of the browser session, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history. With the Kristol reference all of the information with a cookie that has an expired age would be deleted upon termination of the browser, thereby deleting all information pertaining to the cookies and not just the confidential information contained within the cookie.

Additionally, McDonough and Kristol, taken alone or in combination, fail to teach or suggest identifying data elements, within the history, that correspond to the confidential information that has been selected. As discussed above, McDonough teaches that, during a browser session and prior to displaying the requested information a

determination is made as to whether the user has access privileges to the requested information. Kristol teaches removal of information when the age of a cookie expires. Neither reference recognizes the need to identify data elements, within the history (cookie in the Kristol reference), that correspond to the confidential information that has been selected.

Furthermore, there is not so much as a suggestion in either reference to modify the references to include such features. That is, there is no teaching or suggestion in McDonough or Kristol that a problem exists for which receiving a selection of confidential information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser, identifying data elements, within the history, that correspond to the confidential information that has been selected, and responsive to a termination of the browser session, automatically removing the selected confidential information from the history without requiring further user input upon termination of the browser session, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history, is a solution. To the contrary, McDonough only teaches during a browser session, a user may request to view data and, prior to the request being passed to the source, a determination is made whether to pass the request based on the encrypted session state data. Kristol only teaches removal of information when the age of a cookie expires. Neither reference even recognizes a need to receiving a selection of confidential information for removal from a history generated by a browser, identifying data elements within the history that correspond to the confidential information that has been selected and automatically removing the selected confidential information from the history without requiring further user input upon termination of the browser session responsive to a termination of the browser session, as recited in claim 1.

Moreover, neither reference teaches or suggests the desirability of incorporating the subject matter of the other reference. That is, there is no motivation offered in either reference for the alleged combination. The Office Action alleges that the motivation for the combination is "so the user does not have to remember to manually clear confidential data since the system automatically clears the confidential information so that each

session will begin anew, thus protecting the privacy of the user." Neither reference selects confidential information for removal from a history generated by a browser, where the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser. Thus, the only teaching or suggestion to even attempt the alleged combination is based on a prior knowledge of Applicants' claimed invention thereby constituting impermissible hindsight reconstruction using Applicants' own disclosure as a guide.

One of ordinary skill in the art, being presented only with McDonough and Kristol, and without having a prior knowledge of Applicants' claimed invention, would not have found it obvious to combine and modify McDonough and Kristol to arrive at Applicants' claimed invention. To the contrary, even if one were somehow motivated to combine McDonough and Kristol, and it were somehow possible to combine the two systems, the result would not be the invention, as recited in claim 1. The result would be removing information at termination that was identified by age. The resulting system still would not select confidential information for removal from a history generated by a browser, identify data elements, within the history, that correspond to the confidential information that has been selected, and automatically removing the selected confidential information from the history without requiring further user input upon termination of the browser session responsive to a termination of the browser session.

Independent claims 8, 12, 20 and 24 recite similar features in their respective claim terminology. Claim 8, which is representative of the other rejected independent claims 12, 20 and 24, recites "receiving a selection of confidential user information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser; identifying data elements, within the history, that correspond to the confidential information that has been selected; and responsive to generation of the history, removing the selected confidential information from the history, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history."

Thus, McDonough and Kristol, taken alone or in combination, fail to teach or suggest all of the features in independent claims 1, 8, 11, 12, 13, 20, 23 and 24. At least

by virtue of their dependency on claims 1, 8, 13 and 20, McDonough and Kristol, taken alone or in combination, fail to teach or suggest all of the features of dependent claims 2-4, 6, 7, 9, 10, 14-16, 18, 19, 21 and 22. Accordingly, Applicants respectively request withdrawal of the rejection of claims 1-24 under 35 U.S.C. § 103(a).

III. Objection to Claims

The Office Action states that claims 2 and 9 are objected to for containing informalities. Applicants have amended claims 2 and 9 to clarify the subject matter being claimed. Therefore, Applicants respectfully request withdrawal of the objection to the claims.

IV. Conclusion

It is respectfully urged that the subject application is patentable over the prior art of record and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

DATE: June 14, 2004

Francis Lammes

Francis Lammes
Reg. No. 55,353
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 367-2001
Agent for Applicants